PILLAR 4

Secure data

Participating banks only share their transaction and customer data with TMNL and not with each other. The most stringent IT security measures are also implemented to protect data, which are monitored by independent parties. Examples include pseudonymisation, data encryption and access control. Only those employees who require the data for carrying out their duties have access.

What does TMNL do to guarantee the security of data?

TMNL is doing its utmost to ensure data security.The data that banks send to TMNL for processing are secured according to the highest possible standards. TMNL also ensures that privacy-sensitive data cannot be traced back to an individual customer.

How does TMNL receive the data, and how are they secured?

The data are encrypted as part of the data transfer process, as is the connection through which the data are sent. TMNL uses a digital signature to check whether the data were actually sent by the bank and if they were altered before the encrypted data is stored using a separate, secure and encrypted database for each bank. These data can only be accessed for analysis from a highly secure and completely isolated environment. TMNL also records every moment the data is handled, such as requesting or processing the data.

Does TMNL comply with international security standards, and who checks that?

TMNL has an Information Risk Management Framework that is based on five principles of trust: Security, Availability, Integrity of processing, Confidentiality and Privacy. The framework describes all of TMNL's security measures, including their purpose and how they work, in order to limit risks such as the loss of data. An external auditor regularly inspects the framework and checks whether TMNL properly implements all of the security measures described.

Who has access to the data, and how is it monitored?

Only pre-selected TMNL staff have access to the encrypted transaction data. They have been through an exhaustive screening process, and have signed a confidentiality statement and a code of conduct. Each data processing activity, such as a search action, is recorded and can be traced to an individual TMNL employee.

What does TMNL do to protect against attacks from outside?

TMNL uses the latest, most reliable technologies for the best possible security. In addition to the security measures described in the Information Risk Management Framework and the periodic audit by an impartial external party, TMNL also conducts security tests, such as penetration tests, every six months and following major technical alterations. An independent team checks whether the environment is configured correctly and securely.

A team of the best ethical hackers also regularly conducts what are known as 'red team' attacks. The TMNL security team must detect and block these attacks, and TMNL uses the lessons learned to further improve the security of the platform. This is a continuous process.

TMNL has five main pillars that form the basis for everything it says and does.

Read more on tmnl.nl